PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-150360
(43)Date of publication of application : 23.05.2003

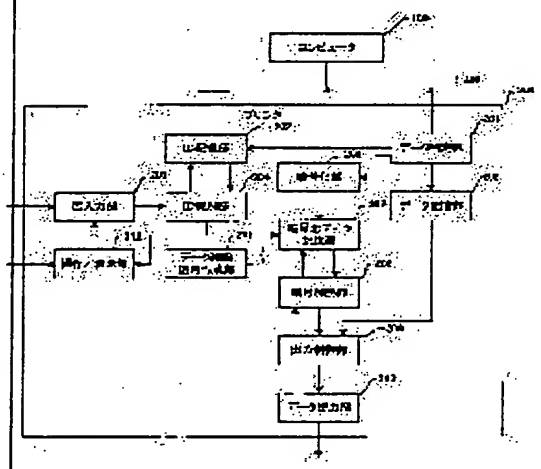
(51)Int.Cl. G06F 3/12
B41J 5/30
B41J 29/00
B41J 29/38
H04N 1/44

(21)Application number : 2001-351205
(22)Date of filing : 16.11.2001

(71)Applicant : RICOH CO LTD
(72)Inventor : NAKAMURA HITOSHI

(54) IMAGE FORMING APPARATUS, SECURITY SYSTEM FOR IMAGE FORMING APPARATUS, SECURITY METHOD FOR IMAGE FORMING APPARATUS AND COMPUTER READABLE STORAGE MEDIUM IN WHICH PROGRAM FOR EXECUTING THE METHOD IS STORED

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image forming apparatus whose safety can be enhanced by a fact that data can not be illegally taken out by deleting the remaining confidential data at the restart and deleting the confidential data when an unauthorized operation is performed.
SOLUTION: The image forming apparatus is provided with a determination part for determining whether or not data received from a computer is the confidential data, a data storage part for storing the confidential data when the received data is determined as the confidential data by the determination part, an ID storage part for storing and managing an ID of the confidential data, an ID discrimination part for discriminating an inputted ID and the ID stored in the ID storage part by comparing them with each other, a data output part for outputting the confidential data stored in the data storage part when the ID inputted by the ID discrimination part is correct and a data deletion control part for deleting the confidential data stored in the data storage part when a system or the image forming apparatus is restarted.



LEGAL STATUS

[Date of request for examination] 26.08.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

③

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－150360
（P2003－150360A）
(43)公開日　平成15年５月23日(2003.5.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｋ	２Ｃ０６１
Ｂ４１Ｊ　5/30		Ｂ４１Ｊ　5/30	Ｚ	２Ｃ０８７
29/00		29/38	Ｚ	５Ｂ０２１
29/38		Ｈ０４Ｎ　1/44		５Ｃ０７５
Ｈ０４Ｎ　1/44		Ｂ４１Ｊ　29/00	Ｚ	

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願2001－351205(P2001－351205)

(22)出願日　平成13年11月16日(2001.11.16)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　中村　仁
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100093920
弁理士　小島　俊郎

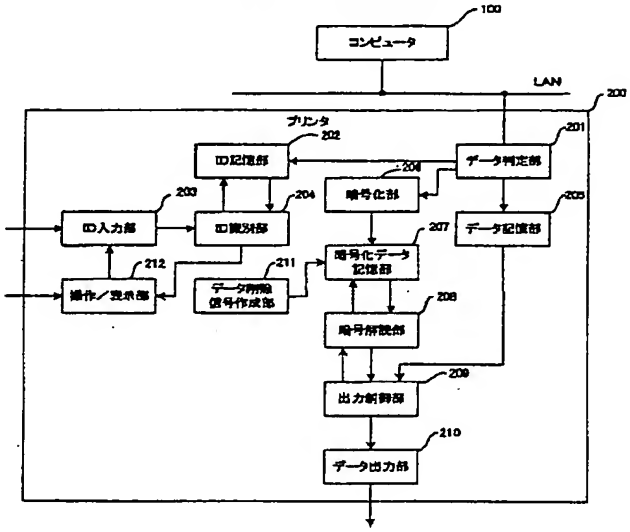
最終頁に続く

(54)【発明の名称】　画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体

(57)【要約】

【解決手段】　本発明は、残った機密データを再起動時に消去することで、また不正操作が行われた場合機密データの消去を行い、データを不正に取り出すことができないことで、安全性を高めることができる画像形成装置を提供することを目的とする。

【解決手段】　本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのＩＤを記憶管理するＩＤ記憶部と、入力されたＩＤとＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、機密データを暗号化する暗号化部と、ＩＤ識別部によって入力されたＩＤが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有する。



1

【特許請求の範囲】

【請求項１】　ホスト側のコンピュータとネットワークを介して接続され、プリンタ、プリント機能を有する複写機及びＦＡＸなどの画像形成装置において、
コンピュータから受信したデータが機密データである否かを判定する判定部と、
該判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、
機密データのＩＤを記憶管理するＩＤ記憶部と、
入力されたＩＤと前記ＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、
機密データを暗号化する暗号化部と、
前記ＩＤ識別部によって入力されたＩＤが正しい場合は前記データ記憶部に記憶された機密データを出力するデータ出力部と、
システム又は画像形成装置が再起動された場合前記データ記憶部に記憶された機密データを消去するデータ消去制御部とを有することを特徴とする画像形成装置。

【請求項２】　前記データ消去制御部は、再起動時に、機密データを消去するか否かを選択する請求項１記載の画像形成装置。

【請求項３】　ＩＤの入力が間違った場合に間違った入力回数をカウントする手段と、間違った入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有する請求項１記載の画像形成装置。

【請求項４】　プリンタ、プリント機能を有する複写機及びＦＡＸなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティシステムにおいて、
コンピュータは、機密データとしてデータを暗号化する際にキーとなるデータとその他のデータとに分割する分割手段と、キーとなるデータとその他のデータを別々に暗号化して記憶する暗号化記憶手段と、消去された機密データを再度出力する場合キーとなるデータのみを作成して画像形成装置に送信するキー作成部とを有し、
画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、該判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのＩＤを記憶管理するＩＤ記憶部と、入力されたＩＤと前記ＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、機密データを暗号化する暗号化部と、前記ＩＤ識別部によって入力されたＩＤが正しい場合は前記データ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合キーとなるデータのみを消去するデータ消去制御部とを有することを特徴とする画像形成装置のセキュリティシステム。

2

【請求項５】　消去された機密データを再度出力する場合前記キー作成部によって作成されたキーよるデータを復元するデータ復元部を有する請求項４記載の画像形成装置のセキュリティシステム。

【請求項６】　画像形成装置は、ＩＤの入力が間違った場合に間違った入力回数をカウントする手段と、間違った入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有する請求項４記載の画像形成装置のセキュリティシステム。

【請求項７】　プリンタ、プリント機能を有する複写機及びＦＡＸなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティ方法において、
機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、保持された機密データを消去することを特徴とする画像形成装置のセキュリティ方法。

【請求項８】　プリンタ、プリント機能を有する複写機及びＦＡＸなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティ方法において、
機密データとしてデータを暗号化する際にキーとその他のデータに分割して各々暗号化し、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、前記キーのみを消去することを特徴とする画像形成装置のセキュリティ方法。

【請求項９】　消去された機密データを再度出力する場合キーを画像形成装置に送信して当該キーよって機密データを復元する請求項８記載の画像形成装置のセキュリティ方法。

【請求項１０】　請求項７～９のいずれかに記載の画像形成装置のセキュリティ方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み出し可能な記憶媒体に関し、詳細にはプリンタ、複写機、ファクシミリ装置及びそれらの各機能を備えた複合機等の画像形成装置により印刷出力される印刷データにおいて、機密指定された印刷データを保護する画像形成装置に関する。

【０００２】

【従来の技術】現在、ホスト側のコンピュータとプリンタ等の出力機器側がネットワーク等で接続されたプリンタシステムにおいて、コンピュータ側から出力されたデータが機密データである場合、当該機密データの漏洩を

防ぐために、機密データをＩＤなどにより出力制御を行って保護し、機密データを一旦保持し、ＩＤにより出力の指示を行う方法が採られている。また、機密データを一旦保持するとき、データの暗号化を行いデータの保護を行っている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来の方法によれば、システムや出力機器の制御に不具合があって再起動を必要とする場合機密データが保持されたままの状態となり、安全性が低くなるという問題点がある。

【０００４】本発明はこの問題点を解決するためのものであり、残った機密データを再起動時に消去することで、また不正操作が行われた場合機密データの消去を行い、データを不正に取り出すことができないことで、安全性を高めることができる、画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】前記問題点を解決するために、ネットワーク環境に接続されたプリンタにおいてシステムや出力機器の不具合により、出力機器の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することより安全性を高める。

【０００６】また、再起動時に消去されるデータを一部として、残りのデータは、部分的にも暗号解読不可能な状態として保持し、再度、消去部分に関してのみの少量のデータの再送することで復元可能とすることで、安全性を高める共に処理の高速化を行う。

【０００７】更に、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにする。

【０００８】

【発明の実施の形態】本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのＩＤを記憶管理するＩＤ記憶部と、入力されたＩＤとＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、機密データを暗号化する暗号化部と、ＩＤ識別部によって入力されたＩＤが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有する。

【０００９】

【実施例】図１は本発明の一実施例に係る画像形成装置のセキュリティシステムの構成を示すブロック図である。なお、本実施例では画像形成装置をプリンタとして説明するものとする。同図において、セキュリティシステムは、主に、コンピュータ１００と、セキュリティ機能を有するプリンタ２００とをＬＡＮを介して接続した構成を有している。また、プリンタ２００は、機密データであるか否かを判定するデータ判定部２０１と、機密データのためのＩＤを管理するＩＤ記憶部２０２と、機密データの出力指示のためのＩＤを入力するＩＤ入力部２０３と、入力されたＩＤを識別するＩＤ識別部２０４と、機密データ以外のデータを出力するためのデータを記憶するデータ記憶部２０５と、機密データを暗号化する暗号化部２０６と、暗号化された機密データを記憶する暗号データ記憶部２０７と、暗号データを解読する暗号解読部２０８と、全てのデータの出力制御を行う出力制御部２０９と、出力データを作像出力するデータ出力部２１０と、機密データを暗号化データ記憶部２０７から削除するためのデータ削除信号を作成するデータ削除信号作成部２１１と、実際にＩＤを入力したり、入力されたＩＤ等や操作ガイダンスを表示する操作／表示部２１２と、更に図示していないが全体の制御をつかさどるＣＰＵとを含んで構成されている。

【００１０】次に、本実施例における機密データを蓄積保持する処理について図１及び機密データ保持動作の動作フローを示す図２に従って説明する。先ず、セキュリティ機能を備えた図１のプリンタ２００が図１のコンピュータ１００からの出力データを受信すると（ステップＳ１０１）、受信したデータが機密データであるか否かを図１のデータ判定部２０１により判定を行う（ステップＳ１０２）。そして、受信したデータが通常のデータである場合、通常のデータ出力のために、一旦データを蓄える図１のデータ記憶部２０５に出力する。データ記憶部２０５は、処理状況により、データを記憶保持あるいは、一時的なバッファとして利用される。保持されたデータは、出力制御部２０９により出力制御される（ステップＳ１０２；ＮＯ、ステップＳ１０３）。一方、出力データが機密データである場合、この出力データは暗号化部２０６により暗号化処理が行われる（ステップＳ１０２；ＹＥＳ、ステップＳ１０４）。暗号化されたデータは、暗号データ記憶部２０７に保持される。暗号化されたデータの保持情報として、記憶場所及びサイズ等を図１のＩＤ記憶部２０２へ出力し、ＩＤ記憶部２０２は、データ受信時に得たＩＤ情報と対応付けて、機密データの記憶場所等の情報と共に記憶管理する（ステップＳ１０５）。

【００１１】次に、本実施例において、出力機器であるプリンタのリセット再起動時の処理について説明すると、このリセット再起動時の処理として、機密データを消去するか否かの情報もＩＤ記憶部２０２により記憶管理する。つまり、図１のＩＤ記憶部２０２での情報管理は、図３に示すように、管理番号、ＩＤ、機密データを

記憶場所（アドレス等）及びサイズ、システム再起動時に機密データの消去するか否かの情報、などの情報の管理を行う。

【００１２】次に、本実施例において、システムの不具合によりシステムの再起動あるいは、プリンタの再起動が行われた場合における機密データの処理方法について図１及び図４に示す動作フローに従って説明する。先ず、システム又はプリンタの再起動が行われると、ＩＤ記憶部２０２により管理されている機密データの情報に基づいて機密データがあるかを調べる（ステップＳ２０１，Ｓ２０２）。機密データがない場合は、データの消去処理は行われない（ステップＳ２０２；ＮＯ、ステップＳ２０３）。一方、機密データがある場合、図１のＩＤ記憶部２０２で記憶管理している機密データの情報に基づいてシステムリセット時の動作を調べる（ステップＳ２０２；ＹＥＳ、ステップＳ２０４）。システムリセット時の動作として、機密データの消去を行わない場合、データの消去処理は行われず、次の機密データの処理を行う（ステップＳ２０４；ＮＯ、ステップＳ２０５）。一方、機密データの消去を行う場合、ＩＤ記憶部２０２で記憶管理している機密データの情報に基づいてそのデータの記憶場所（アドレス）を調べ、図１の暗号データ記憶部２０７に記憶されている機密データの消去をデータ削除信号作成部２１１の制御により消去を行う（ステップＳ２０４；ＹＥＳ、ステップＳ２０６）。また、ＩＤ記憶部２０２の情報も削除する（ステップＳ２０７）。この処理を機密データ全てに関して、繰り返し行うことで、リセット再起動時に、機密データの消去が可能である。

【００１３】図５は本実施例における機密データとｋｅｙデータの蓄積の処理フローを示すフローチャートである。同図において、先ず機密データの出力命令が図１のコンピュータ１００より出力されると、コンピュータ１００は、機密データをｋｅｙとその他のデータに分割する（ステップＳ３０１，Ｓ３０２）。そして、プリンタ２００へ分割したｋｅｙデータとその他のデータを送信する（ステップＳ３０３）。プリンタ２００は、コンピュータ１００からのデータを受信し、受信したデータが機密データである否か判断する（ステップＳ３０４、ステップＳ３０５）。そして、機密データでない場合は、通常データとして出力を行う（ステップＳ３０５；ＮＯ、ステップＳ３０６）。一方、機密データである場合は、ｋｅｙデータとその他のデータをそれぞれ暗号化される（ステップＳ３０５；ＹＥＳ、ステップＳ３０７）。そして、暗号化されたｋｅｙデータとその他のデータを蓄積する（ステップＳ３０８）。なお、機密データの情報管理として、図６に示すように、データの登録番号、ＩＤ番号、機密データのｋｅｙ以外の暗号化データの記憶場所（アドレス）、データのサイズ、ｋｅｙデータの記憶場所（アドレス）、起動時にデータを消去する否かの判断の情報を管理記憶する。

【００１４】次に、本実施例において、システムの再起動あるいは、プリンタの再起動が行われた場合における機密データのｋｅｙデータの消去及び消去された状態から機密データを復元する処理について図１及び図７に示す動作フローに従って説明する。先ず、システム又はプリンタが再起動されると、図１のＩＤ記憶部２０２にて記憶管理されている情報より、機密データの有無を調べる（ステップＳ４０１，Ｓ４０２）。機密データがない場合、機密データの消去処理は終了となる（ステップＳ４０２；ＮＯ、ステップＳ４０３）。一方、機密データがある場合、起動時のデータ消去を行うか否かの情報を調べる（ステップＳ４０２；ＹＥＳ、ステップＳ４０４）。そして、起動時のデータ消去を行わない場合、次のデータの処理を行う（ステップＳ４０４；ＮＯ、ステップＳ４０５）。一方、起動時のデータ消去を行う場合、ｋｅｙデータ部分のみ消去する（ステップＳ４０４；ＹＥＳ、ステップＳ４０６）。また、ＩＤ記憶部情報のｋｅｙ情報を削除する（ステップＳ４０７）。なお、ｋｅｙ情報の削除は、図７に示すように、管理番号０００３のｋｅｙデータのアドレスを“ｅｅｅｅｅｅｅ”のように特定の値とする。この特定の値により、ｋｅｙが削除されたものとする。上記一連の処理を全機密データに対して繰り返し行う。

【００１５】次に、本実施例におけるｋｅｙが削除されたデータを再度出力する処理について当該処理フローを示す図８に従って説明する。先ず、再起動されたシステムにおいてｋｅｙが消去されたデータを出力するために、消去された機密データの再送の指示する（ステップＳ５０１）。コンピュータ１００側は、データからｋｅｙとなるデータを作成する（ステップＳ５０２）。ここで、出力機器であるプリンタ２００中のｋｅｙデータと、コンピュータ１００が作成するｋｅｙデータと一致するように指示して作成する。なお、ｋｅｙデータの作り方は、指示することにより、作成データを変更可能とする。その後、出力機器であるプリンタ２００へデータを送信する（ステップＳ５０３）。出力機器であるプリンタ２００側は、受信したデータが機密データであるか否か判断を行う（ステップＳ５０４）。機密データでない場合は、通常出力処理を行う（ステップＳ５０４；ＮＯ、ステップＳ５０５）。一方、機密データである場合は、受信したデータがｋｅｙによるデータの復元であるか否か判断する（ステップＳ５０４；ＹＥＳ、ステップＳ５０６）。ｋｅｙによる復元でない場合、機密データとしてデータの蓄積を行う（ステップＳ５０６；ＮＯ、ステップＳ５０７）。一方、ｋｅｙによる復元である場合、ｋｅｙデータの暗号化を行い、データを蓄積する。また、ＩＤデータ記憶部の情報を該当する機密データの情報の復元して記憶する（ステップＳ５０６；ＹＥＳ、ステップＳ５０８，Ｓ５０９）。以上の一連の処理で、

ｋｅｙに関するデータ及び情報を復元し、機密データの出力が可能な状態となる。

【００１６】次に、本実施例における出力機器であるプリンタから機密データの出力要求がＩＤの入力が不正である場合にデータの保護のため機密データを削除する処理について当該処理フローを示す図９に従って説明する。なお、一例として、不正に出力指示した回数によりデータを消去する処理手順を説明する。

【００１７】先ず、出力機器である図１のプリンタ２００の操作／表示部２１２より機密データの出力指示がされると、ＩＤの入力を促すメッセージを表示し、ＩＤの入力待ちとなる（ステップＳ６０１，Ｓ６０２）。そして、ＩＤが入力されると、ＩＤに該当する機密データが保持されているか否か判断する（ステップＳ６０３，Ｓ６０４）。該当するデータが存在する場合は、機密データを読み出し、暗号解読処理を行って、データのプリントアウトを行う（ステップＳ６０４；ＹＥＳ、ステップＳ６０５～Ｓ６０７）。一方、該当するデータが存在しない場合、不正に機密データを出力させようとしているものと判断する。不正と判断した場合をカウントする（ステップＳ６０４；ＮＯ、ステップＳ６０８）。そして、不正と判断した回数が設定した所定値以上でない場合、指示待ちの状態に戻る（ステップＳ６０９；ＮＯ）。一方、不正と判断した回数が設定した所定値以上である場合、機密データの消去を行う（ステップＳ６０９；ＹＥＳ、ステップＳ６１０）。なお、機密データの消去方法は、前述のように行う。

【００１８】次に、図１０は本発明のシステム構成を示すブロック図である。つまり、同図は上記実施例における画像形成装置のセキュリティ方法によるソフトウェアを実行するマイクロプロセッサ等から構築されるハードウェアを示すものである。同図において、画像形成装置のセキュリティシステムはインターフェース（以下Ｉ／Ｆと略す）１０１、ＣＰＵ１０２、ＲＯＭ１０３、ＲＡＭ１０４、表示装置１０５、ハードディスク１０６、キーボード１０７及びＣＤ－ＲＯＭドライブ１０８を含んで構成されている。また、汎用の処理装置を用意し、ＣＤ－ＲＯＭ１０９などの読取可能な記憶媒体には、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶されている。更に、Ｉ／Ｆ１０１を介して外部装置から制御信号が入力され、キーボード１０７によって操作者による指令又は自動的に本発明のプログラムが起動される。そして、ＣＰＵ１０２は当該プログラムに従って上述の画像形成装置のセキュリティ方法に伴う制御処理を施し、その処理結果をＲＡＭ１０４やハードディスク１０６等の記憶装置に格納し、必要により表示装置１０５などに出力する。以上のように、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶した媒体を用いることにより、既存のシステムを変えることなく、画像形成装置のセキュリティシステムを

汎用的に構築することができる。

【００１９】なお、本発明は上記実施例に限定されるものではなく、特許請求の範囲内の記載であれば多種の変形や置換可能であることは言うまでもない。

【００２０】

【発明の効果】以上説明したように、本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのＩＤを記憶管理するＩＤ記憶部と、入力されたＩＤとＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、機密データを暗号化する暗号化部と、ＩＤ識別部によって入力されたＩＤが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有することに特徴がある。よって、ネットワーク環境に接続されたプリンタ等の画像形成装置においてシステムや画像形成装置の不具合により、システム又は画像形成装置の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【００２１】また、データ消去制御部は、再起動時に、機密データを消去するか否かを選択することにより、画像形成装置側で機密データの出力を管理することができる。

【００２２】更に、ＩＤの入力が間違った場合に間違った入力回数をカウントする手段と、間違った入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有することにより、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにすることができる。

【００２３】また、別の発明としての画像形成装置のセキュリティシステムによれば、コンピュータは、機密データとしてデータを暗号化する際にキーとなるデータとその他のデータとに分割する分割手段と、キーとなるデータとその他のデータを別々に暗号化して記憶する暗号化記憶手段と、消去された機密データを再度出力する場合キーとなるデータのみを作成して画像形成装置に送信するキー作成部とを有し、画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのＩＤを記憶管理するＩＤ記憶部と、入力されたＩＤとＩＤ記憶部に記憶されたＩＤとを比較して識別するＩＤ識別部と、機密データを暗号化する暗号化部と、ＩＤ識別部によって入力されたＩＤが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動され

た場合キーとなるデータのみを消去するデータ消去制御部とを有する。よって、このような構成を有するセキュリティシステムによれば、ネットワーク環境に接続されたプリンタ等の画像形成装置においてシステムや画像形成装置の不具合により、システム又は画像形成装置の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【００２４】また、消去された機密データを再度出力する場合キー作成部によって作成されたキーよるデータを復元するデータ復元部を有することにより、再起動時に消去されるデータを一部として、残りのデータは、部分的にも暗号解読不可能な状態として保持し、再度、消去部分に関してのみの少量のデータの再送することで復元可能とすることで、安全性を高める共に処理の高速化を図ることができる。

【００２５】更に、セキュリティシステムにおける画像形成装置は、ＩＤの入力が間違った場合に間違った入力回数をカウントする手段と、間違った入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有することにより、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにすることができる。

【００２６】また、別の発明として画像形成装置のセキュリティ方法によれば、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、保持された機密データを消去する。よって、機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【００２７】更に、機密データとしてデータを暗号化する際にキーとその他のデータに分割して各々暗号化し、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、キーのみを消去することにより、機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【００２８】また、消去された機密データを再度出力する場合キーを画像形成装置に送信して当該キーよって機密データを復元することにより、安全性を高める共に処理の高速化を図ることができる。

【００２９】更に、上記記載の画像形成装置のセキュリティ方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体に特徴がある。よって、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶した媒体を用いることにより、既存のシステムを変えることなく、画像形成装置のセキュリティシステムを構築する装置を汎用的に使用することができる。

【図面の簡単な説明】

【図１】本発明の一実施例に係る画像形成装置のセキュリティシステムの構成を示すブロック図である。

【図２】本実施例における機密データ保持動作を示すフローチャートである。

【図３】図１のＩＤ記憶部での情報管理内容を示す図である。

【図４】再起動時の機密データの処理を示すフローチャートである。

【図５】本実施例における機密データとｋｅｙデータの蓄積の処理フローを示すフローチャートである。

【図６】図１のＩＤ記憶部での別の情報管理内容を示す図である。

【図７】本実施例における再起動時の機密データのｋｅｙデータの消去及び消去された状態から機密データを復元する処理を示すフローチャートである。

【図８】本実施例におけるｋｅｙが削除されたデータを再度出力する処理を示すフローチャートである。

【図９】本実施例における出力機器であるプリンタから機密データの出力要求がＩＤの入力が不正である場合にデータの保護のため機密データを削除する処理を示すフローチャートである。

【図１０】本発明のシステム構成を示すブロック図である。

【符号の説明】

１００；コンピュータ、２００；プリンタ、２０１；データ判定部、２０２；ＩＤ記憶部、２０３；ＩＤ入力部、２０４；ＩＤ識別部、２０５；データ記憶部、２０６；暗号化部、２０７；暗号化データ記憶部、２０８；暗号解読部、２０９；出力制御部、２１０；データ出力部、２１１；データ削除信号作成部、２１２；操作／表示部。

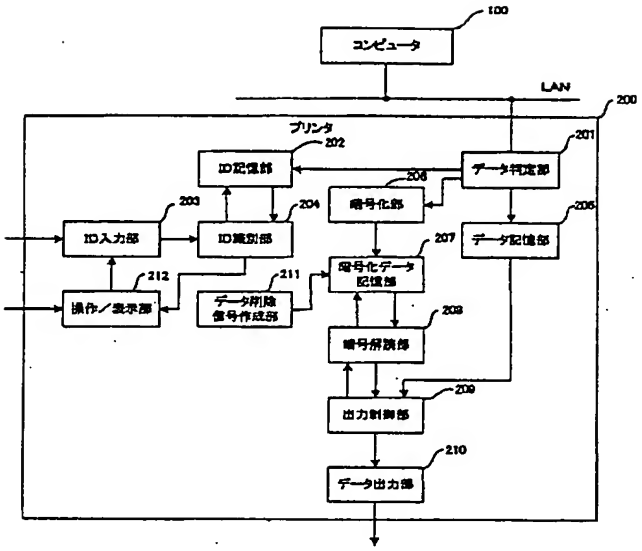
【図３】

管理番号	ID	データ記憶アドレス	サイズ	起動時データ消去
0001	abc12346	1000000	xxxx	1
0002	abc12345	1002000	xxxx	0
0003		1004000		

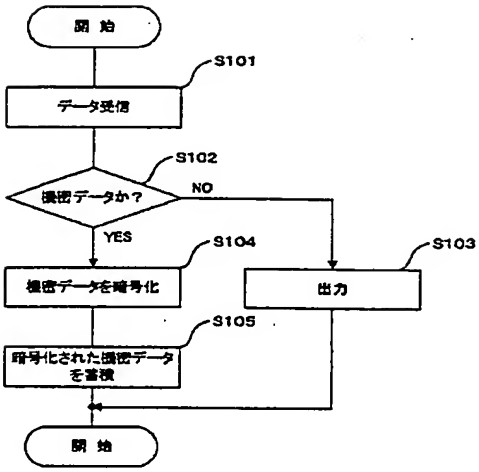
【図７】

管理番号	ID	データ記憶アドレス	Keyデータアドレス	サイズ	起動時データ消去
0001	abc12346	1000000	a000000	xxxx	1
0002	abc12345	1002000	a0001000	xxxx	0
0003	abc11111	1004000	eeeeeee		

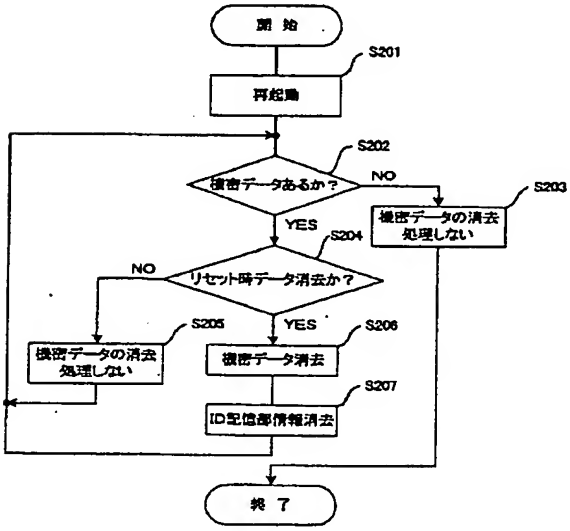
【図１】


100
コンピュータ
LAN
200
プリンタ
202
ID記憶部
201
データ判定部
206
暗号化部
203
ID入力部
204
ID識別部
205
データ記憶部
207
暗号化データ記憶部
212
操作／表示部
211
データ削除信号作成部
208
暗号解読部
209
出力制御部
210
データ出力部

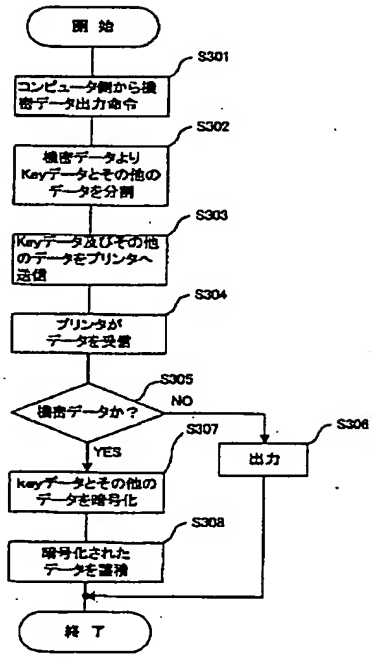
【図２】


開 始
S101
データ受信
S102
機密データか？
NO
YES
S104
機密データを暗号化
S103
出力
S105
暗号化された機密データを蓄積
開 始

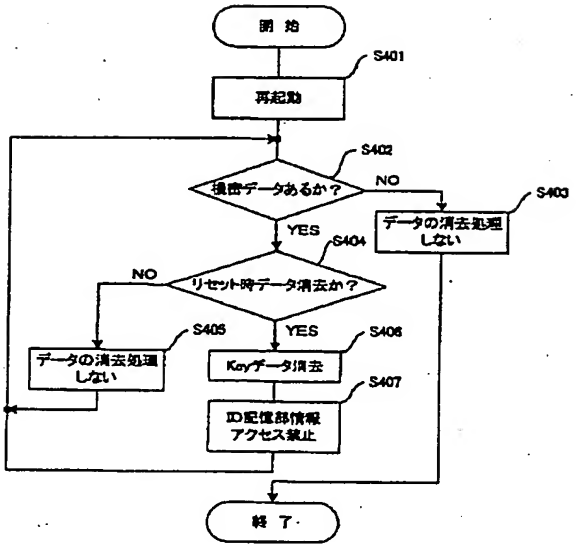
【図４】


開 始
S201
再起動
S202
機密データあるか？
NO
S203
機密データの消去処理しない
YES
S204
リセット時データ消去か？
NO
YES
S205
機密データの消去処理しない
S206
機密データ消去
S207
ID記憶部情報消去
終 了

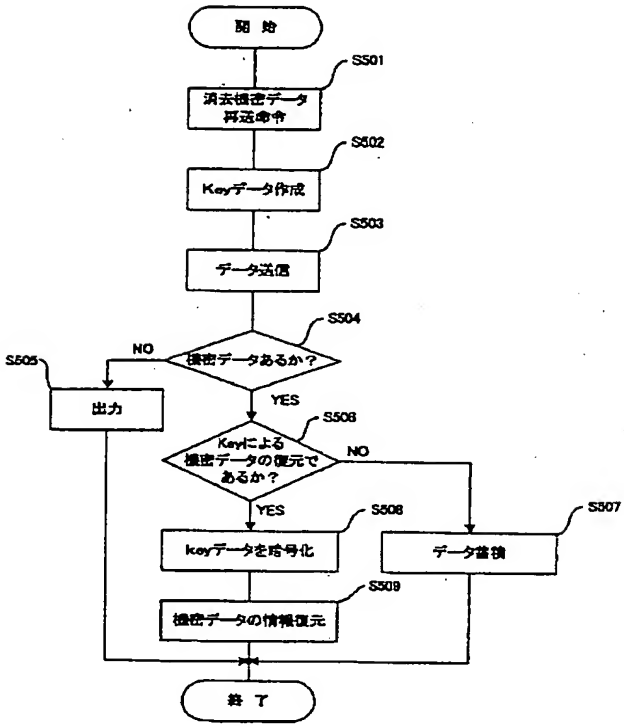
【図５】


開 始
S301
コンピュータ側から機密データ出力命令
S302
機密データよりKeyデータとその他のデータを分割
S303
Keyデータ及びその他のデータをプリンタへ送信
S304
プリンタがデータを受信
S305
機密データか？
NO
S306
出力
YES
S307
keyデータとその他のデータを暗号化
S308
暗号化されたデータを蓄積
終 了

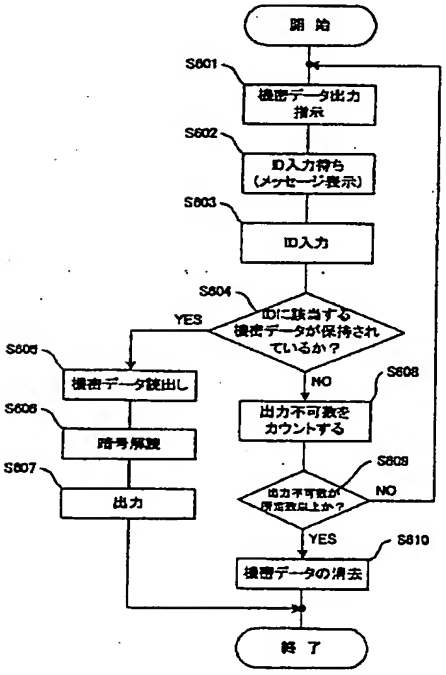
【図６】


開 始
S401
再起動
S402
機密データあるか？
NO
S403
データの消去処理しない
YES
S404
リセット時データ消去か？
NO
YES
S405
データの消去処理しない
S406
Keyデータ消去
S407
ID記憶部情報アクセス禁止
終 了

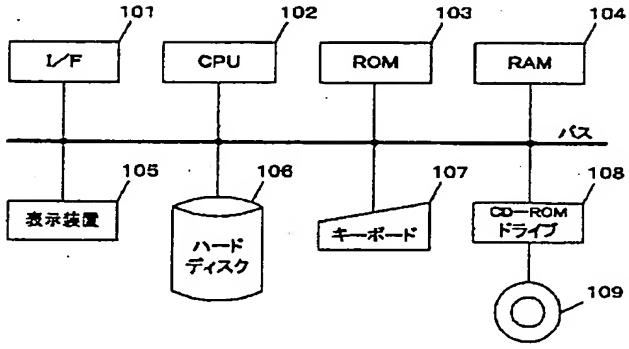
【図８】


開 始
S501
消去機密データ再送命令
S502
Keyデータ作成
S503
データ送信
S504
機密データあるか？
NO
S505
出力
YES
S506
Keyによる機密データの復元であるか？
NO
YES
S508
keyデータを暗号化
S507
データ蓄積
S509
機密データの情報復元
終 了

【図９】


開 始
S601
機密データ出力指示
S602
ID入力待ち(メッセージ表示)
S603
ID入力
S604
YES
IDに該当する機密データが保持されているか？
NO
S605
機密データ読出し
S606
暗号解読
S607
出力
S608
出力不可数をカウントする
S609
出力不可数が所定数以上か？
NO
YES
S610
機密データの消去
終 了

【図１０】


101
I/F
102
CPU
103
ROM
104
RAM
バス
105
表示装置
106
ハードディスク
107
キーボード
108
CD-ROMドライブ
109

フロントページの続き

Fターム(参考) 2C061 AP01 AP03 AP04 AP07 BB17
CL08 CL10 HJ06 HK23 HN23
2C087 AA03 AA09 AB05 BA14 BC04
BC06 DA13
5B021 AA02 BB01 BB04 BB09 CC05
5C075 AA90 AB90 EE02 EE03 EE90
FF90